

## CLAIMS

What is claimed is:

1. A method of configuring an open interoperable security assertions markup language (SAML) session comprising:

5       receiving a first entity identifier of a first entity by a second entity;

          receiving a first account mapping between said first entity and said second entity by said second entity;

          storing said first entity identifier and said first account mapping as a first record in a first partner list accessible to said second entity;

10       receiving a second entity identifier of said second entity by said first entity;

          receiving a second account mapping between said second entity and said first entity by said first entity; and

          storing said second entity identifier and said second account mapping as a second record in a second partner list accessible to said first entity.

15

2. The method according to Claim 1, wherein said first account mapping is implemented as a java class.

3. The method according to Claim 1, wherein said first account mapping defines a mapping of a subject between said second entity and said first entity.

20

4. The method according to Claim 1, further comprising:

receiving one or more mappings between said first entity and said second entity by said second entity, wherein the mappings are selected from the group consisting of an attribute mapping, a site attribute list, an account mapping, and an action mapping;

storing said one or more mappings between said first entity and said second entity as  
5 a part of said first record in said first partner list accessible to said second entity;

receiving one or more mappings between said second entity and said first entity by said first entity, wherein the mappings are selected from the group consisting of an attribute mapping, a site attribute list, an account mapping, and an action mapping; and

storing said one or more mappings between said second entity and said first entity as  
10 part of said second record in said second partner list accessible to said first entity.

5. The method according to Claim 4, wherein said attribute mapping, said site attribute list, said account mapping, and said action mapping are implemented as a java class.

15 6. The method according to Claim 4, wherein said attribute mapping defines a mapping of an attribute between said second entity and said first entity.

7. The method according to Claim 4, wherein said site attribute list defines a list of attribute to be exchanged between said second entity and said first entity.

20

8. The method according to Claim 4, wherein said action mapping defines a mapping of an authorization of said second entity to an authorization of said first entity.

9. The method according to Claim 1, further comprising:  
receiving a first client certificate of said first entity by said second entity;  
receiving a first network address of said first entity by said second entity;  
5 storing said first client certificate and said first network address as another part of said  
first record in said first partner list accessible to said second entity;  
receiving a second client certificate of said second entity by said first entity;  
receiving a second network address of said second entity by said first entity; and  
storing said second client certificate and said second network address as another part  
10 of said second record in said second partner list accessible to said first entity.

10. A method of providing an open interoperable security assertions markup language  
(SAML) session comprising:  
receiving a SAML request, comprising an entity identifier, by a first entity;  
15 searching a partner list of said first entity for a record containing a matching entity  
identifier, wherein said record contains an account mapping; and  
processing said SAML request in accordance with said account mapping.

11. The method according to Claim 10, wherein said account mapping defines a  
20 mapping of an account of said second entity to an account of said first entity.

12. The method according to Claim 10, further comprising:

searching a partner list of said first entity for a record containing a matching entity identifier, wherein said record contains an attribute mapping; and  
processing said SAML assertion in accordance with said attribute mapping.

5           13. The method according to Claim 12, wherein said attribute mapping defines a mapping of an attribute of said second entity to said first entity.

14. The method according to Claim 12, wherein said attribute mapping defines a mapping of an attribute namespace of said second entity to said first entity.

10

15. The method according to Claim 10, further comprising:

searching a partner list of said first entity for a record containing a matching entity identifier, wherein said record contains an action mapping; and  
processing said SAML assertion in accordance with said action mapping.

15

16. The method according to Claim 15, wherein said action mapping defines a mapping of an authorization decision of said second entity to an authorization decision of said first entity.

20           17. The method according to Claim 10, further comprising sending a SAML assertion in response to said SAML request.

18. The method according to Claim 17, further comprising:

searching a partner list of said first entity for a record containing a matching entity identifier, wherein said record contains a site attribute list; and  
generating said SAML assertion in accordance with said site attribute list.

5

19. The method according to Claim 18, wherein said site attribute list defines an attribute that is to be returned by said second entity to said first entity.

20. A system for configuring an open and interoperable security assertions markup language (SAML) session comprising:

a first entity comprising;

a first administration module for receiving a first entity identifier of a second entity and a first account mapping between said second entity and said first entity; and

15 a first partner list, accessible by said first administration module, for storing said first entity identifier and said first account mapping; and

said second entity comprising;

a second administration module for receiving a second identifier of said first entity and a second account mapping between said first entity and said second entity; and

20

a second partner list, accessible by said second administration module, for storing said second entity identifier and said second account mapping.

21. The system according to Claim 20, wherein said first account mapping defines a mapping of a subject between said second entity and said first entity.

5        22. The system according to Claim 20, wherein:

      said first administration module receives a first attribute mapping between said second entity and said first entity;

      said first partner list stores said first attribute mapping;

      said second administration module receives a second attribute mapping between said  
10    first entity and said second entity; and

      said second partner list stores said second attribute mapping.

23. The system according to Claim 22, wherein said attribute mapping defines a mapping of an attribute of said second entity to said first entity.

15

24. The system according to Claim 20, wherein:

      said first administration module receives a first site attribute list between said second entity and said first entity;

      said first partner list stores said first site attribute list;

20        said second administration module receives a second site attribute list between said first entity and said second entity; and

      said second partner list stores said second site attribute list.

25. The system according to Claim 24, wherein said site attribute list defines an attribute that is to be returned by said second entity to said first entity.

5           26. The system according to Claim 20, wherein:  
            said first administration module receives a first action mapping between said second entity and said first entity;  
            said first partner list stores said first action mapping;  
            said second administration module receives a second action mapping between said  
10   first entity and said second entity; and  
            said second partner list stores said second action mapping.

            27. The system according to Claim 26, wherein said action mapping defines a mapping of an authorization decision of said second entity to an authorization decision of  
15   said first entity.

            28. A system for providing an open and interoperable security assertions markup language (SAML) session comprising:  
            a first entity comprising  
20           a first session module for generating and sending a SAML request; and

a first partner list, accessible by said first session module, comprising a first plurality of records each comprising an entity identifier and a corresponding account mapping; and

a second entity, communicatively coupled to said first entity, comprising;

5 a second session module for receiving and processing said SAML request in accordance with an account mapping between said second entity and said first entity; and

a second partner list, accessible by said second session module, comprising a second plurality of records each comprising an entity identifier and a  
10 corresponding account mapping.

29. The system according to Claim 28, wherein said second session module looks-up an entity identifier contained in said SAML request in said partner list to determine said account mapping.

15

30. The system according to Claim 28, wherein said second partner list further comprises an attribute mapping between said first entity and said second entity, and wherein said SAML request is further processed according to said attribute mapping.

20 31. The system according to Claim 28, wherein said second partner list further comprises an action mapping between said first entity and said second entity, and wherein said SAML request is further processed according to said action mapping.

32. The system according to Claim 28, wherein said first partner list further comprises a site attribute list between said first entity and said second entity, and wherein said second session module generates a SAML assertion in accordance with said site attribute  
5 list.

33. A computer readable-medium containing a plurality of instructions which when executed cause a network device to implement a method of providing an open and interoperable single sign-on session comprising:

10 receiving a first entity identifier, a first account mapping, a first attribute mapping, a first site attribute list and a first action mapping by said second entity;

storing said first entity identifier, said first account mapping, said first attribute mapping, said first site attribute list and said action mapping as a first record in a first partner list accessible to said second entity;

15 receiving a second entity identifier, a second account mapping, a second attribute mapping, a second site attribute list and a second action mapping by said first entity; and

storing said second entity identifier, said second account mapping, said second attribute mapping, said second site attribute list and said second action mapping as a second record in a second partner list accessible to said first entity.

20

34. The computer readable-medium according to Claim 33, further comprising:

receiving a security assertions markup language (SAML) request, comprising said second entity identifier of said second entity, by a first entity;

retrieving said second account mapping by matching said second entity identifier received in said SAML request with said second entity identifier in said second record; and  
5 processing said SAML request in accordance with said account mapping.

35. The computer readable-medium according to Claim 33, further comprising:

retrieving said second attribute mapping by matching said second entity identifier received in said SAML request with said second entity identifier in said second record; and  
10 processing said SAML request in accordance with said attribute mapping.

36. The computer readable-medium according to Claim 33, further comprising:

retrieving said second action mapping by matching said second entity identifier received in said SAML request with said second entity identifier in said second record; and  
15 processing said SAML request in accordance with said attribute mapping.

37. The computer readable-medium according to Claim 33, further comprising:

retrieving said second site attribute list by matching said second entity identifier received in said SAML request with said second entity identifier in said second record; and  
20 generating said SAML assertion in accordance with said site attribute list.

38. The computer readable-medium according to Claim 33, wherein said second account mapping defines a mapping of a subject between said first entity and said second entity.

5           39. The computer readable-medium according to Claim 33, wherein said second attribute mapping defines a mapping of an attribute between said first entity and said second entity.

40. The computer readable-medium according to Claim 33, wherein said second site  
10 attribute list defines an attribute to be exchanged between said first entity and said second entity.

41. The computer readable-medium according to Claim 33, wherein said second action  
mapping defines a mapping of an authorization decision of said first entity to and  
15 authorization decision of said second entity.